양자 내성 암호 연구 동향 분석

최여정, 이만희*
한남대학교, *한남대학교
choiyeojeong98@gmail.com, *manheelee@hnu.kr

Analysis of Post-Quantum Cryptography Research Trends

Yeo-Jeong Choi, Man-Hee Lee*
Hannam Univ., *Hannam Univ.

요 약

기존 컴퓨터의 성능은 미세공정을 통해 기하급수적인 발전을 하였다. 하지만 성능 저하 문제로 인해 한계에 다다랐고 이를 대체하기 위해 미국 IT 주요 기업을 주축으로 양자 컴퓨터가 발전하고 있다. 양자 컴퓨터는 많은 양의 연산을 동시에 처리할 수 있어 양자 알고리즘 구현 가능성을 증가시킨다. 또한, 정수를 기반으로 한 문제에 대해 뛰어난 연산 능력을 보여 수학적 난제에 기반하고 있는 기존의 암호 체계를 위협하고 있다. 따라서 양자 알고리즘으로부터 안전하고 기존의 암호 체계를 대신할 수 있는 양자 암호 기술이 필요하다. 양자 내성 암호(PQC, Post-Quantum Cryptography)는 양자 컴퓨터의 연산 능력으로 풀기 어려운 수학 문제를 기반한 새로운 암호 체계로 주목받고 있다. 그에 따라 본 논문은 양자 알고리즘으로부터 안전한 양자 암호 기술인 양자 내성 암호(PQC, Post-Quantum Cryptography)의 연구 동향을 소개한다.

Ⅰ. 서 론

기존 컴퓨터의 성능은 트랜지스터의 미세공정을 통해 기하급수적으로 발전해 왔다. 하지만 지속적인 트랜지스터의 크기 축소는 터널링 현상 등으로 인한 성능 저하 문제가 발생하므로 많은 전문가는 기존 컴퓨터의 발전이 한계에 다다랐다고 판단하고 있다[1]. 이에 Google, IBM, IonQ 등 미국 주요 IT 기업들은 기존 컴퓨터를 대체하여 양자컴퓨터를 개발하고 있다.

동시에 많은 양의 연산을 처리할 수 있는 양자 컴퓨터가 개발됨에 따라 소인수분해와 같이 수학적 연산량에 의존하는 기존의 암호 체계를 위협하고 있다. Shor 알고리즘은 소인수분해를 효율적으로 계산하는 양자 알고리즘으로, 다항 시간 안에 연산이 가능해짐에 따라 RSA 및 ECC 기반 공개키 암호 시스템의 효과적인 공격이 가능해진다[2]. 또한, Grover 알고리즘은 블랙박스 함수 입력값을 높은 확률로 찾는 양자 알고리즘이다. 비정형 검색에 효율적이며, 기존 알고리즘에 비해 조건을 만족하는 미지의 값을 쉽게 찾을 수 있다[3]. 이처럼 기존 암호 체계를 위협하는 양자 알고리즘의 구현 가능성이 증가하고 있음에 따라 양자 컴퓨팅으로부터 안전한 양자 암호 기술이 필요하다.

PQC(Post-Quantum Cryptography)는 양자 알고리즘에 의해 해독 가능성이 존재하는 기존 암호 체계를 대신하기 위해 고안된 공개키 양자 암호 기술로, 양자 컴퓨터의 연산 능력으로 풀기 어려운 수학 문제에 기반하여 만들어졌다. 이에 따라 정수 기반 문제에 뛰어난 성능을 보이는 양자 컴퓨터에 대해 다항 시간 내에 쉽게 해독되지 않을 것으로 기대되어 새로운 암호 체계로 주목받고 있다. PQC의 종류에는 다변수 기반(Multivariate-based) 암호, 코드 기반(Code-based) 암호, 격자 기반(Lattice-based) 암호, 아이소 제니 기반(Isogeny-based) 암호, 해시 기반(Hash-based) 암호 알고리즘이 있다[4][5].

본 논문에서는 기존 암호 체계를 대신하면서 양자 알고리즘으로부터 안전한 PQC의 국내외 연구 동향을 소개한다. 그 후 우리가 가지고 있는 양자 내성 암호의 활발한 연구 필요성을 강조하며 결론 맺는다.

Ⅱ. 국내 양자 내성 암호 연구 동향

2.1 국가 수리 연구소

2020년 4월, 국가 수리 연구소의 암호 기술 연구팀은 새로운 수학적 난제인 다변수 이차식 문제를 기반으로 한 공개키 암호 알고리즘을 개발하였다. 해당 알고리즘은 리소스(resource) 제한으로 인해 경량 IoT 기기에서 속도가 월등히 느린 국제표준 공개키 암호 RSA와 ECDSA의 단점을 보완한 것으로, 경량 IoT 기기에서 고속 구현이 가능하며 양자 알고리즘인 Shor 알고리즘으로부터 안전한 것으로 밝혀졌다[5]. 또한, 공개키 암호의 키 생성 속도는 국제 표준 전자 서명 알고리즘인 ECDSA-256와 비교하여 36배 빠르고 다변수 기반의 레인보우 알고리즘과 비교해도 빠른 속도를 보였다. 해당 알고리즘은 AI를 활용한 다양한 스마트 환경에서 기기 인증으로 활용될 것으로 예측되며, 현재 블록체인에서 사용하는 국제표준 전자서명인 ECDSA 대신 사용될 것으로 기대하고 있다[6][7].

2.2 LG유플러스

LG유플러스는 다수의 대학, 기관 및 기업과 협업하여 양자 내성 암호를 개발하고 실생활에 적용하고 있다. 서울대학교 산업 수학 센터와 크립토랩이 공동으로 양자 내성 암호 기술을 적용한 광통신 전용망 장비를 개발하였고, 코위버와의 협력을 통해 세계 최초로 양자 내성 암호를 광전송장비 ROADM에 활용하는 등 광통신의 양자 내성 암호 사용 범위를 넓혀가고 있다. 또한, 다량의 데이터를 전송하는 의료분야의 시스템 보안을 강화하기 위해 보안 전문 회사 ICTK 홀딩스와 을지대학교병원의 의료정보시스템에 양자 내성 암호 기술을 결합한 앱을 개발하였다. V2X 통신 인프라 보안을 위해 양자 내성 암호를 보안 인증 체계 및 오픈랩에 적용하는 등 실생활에서의 양자 내성 암호의 적용 범위를 다방면으로 넓히고 있다[5][8].

2.3 ㈜드림시큐리티

2017년 4월, ㈜드림시큐리티는 양자 내성 암호 및 암호 키 관련 기술 등

차세대 암호 기술을 확보하기 위해 '암호 기술 연구센터'를 설립하였다. 또한, 격자 기반 양자 내성 키 알고리즘 Lizard 등 국내 표준 알고리즘을 적용한 보안 제품을 개발하며 지속적으로 보완하고 있다[9].

Ⅲ. 국외 양자 내성 암호 연구 동향

3.1 구글(Google)

2016년, 구글(Google)은 양자 컴퓨터의 공격으로부터 기밀성을 유지하기 위해 양자 내성 암호 CECPQ1을 개발하여 웹브라우저 카나리아에 적용하였다. 이는 격자 기반 암호 키 교환 프로토콜인 New Hope과 타원곡선 디피헬만 키교환 ECDHE(Elliptic Curve Diffie-Hellman Exchange)를 결합한 것으로, 추후에 개발될 양자 컴퓨터에 대응하고 안정성을 높이기 위해 기업에서 양자 내성 암호를 적용한 대표적인 사례로 볼 수 있다[5]. 그 후 실제 사용자 장치에서 사용되는 양자 키 교환 알고리즘 성능의 실험적 평가를 위해 CECPQ2가 개발되었다. 이는 타원곡선 디피헬만 키 교환 X25519와 격자 기반 HRSS 알고리즘을 사용한다[10].

3.2 미국 국립표준 기술 연구소(NIST)

2016년, 미국 국립표준 기술 연구소(NIST, National Institute of Standards and Technology)는 양자 컴퓨터의 공격에도 안전한 암호 알고리즘을 선정하기 위해 양자 내성 암호의 표준 공모를 시작하였다. 안전성, 성능, 인터넷 프로토콜과의 연동 가능성 등을 평가하며 2020년 7월, 양자 내성 암호 3차 선정 결과를 발표하였다[11].

3.3 Infineon Technologies

2017년, 독일 기업 Infineon Technologies는 최초로 비접촉 스마트카드에 격자 기반 암호 키 교환 프로토콜인 New Hope을 적용하였고, 이를 통해 송·수신자 간의 암호화된 채널을 사용할 수 있게 하였다. 구현 과정 중 제한된 메모리, 트랜잭션 속도 등 제한이 많았으나 SESAMES Award의 사이버보안(Cybersecurity), 전자정부(eGovernment) 두 부문을 수상하며 성공적인 결과를 도출했다[12][13]. 이는 국제표준 공개키 암호(RSA, ECC) 수준의 안전성을 제공하며 양자 컴퓨터의 연산 능력으로 풀기 어렵다는 특징이 있다[5].

Ⅳ. 정리 및 시사점

(그림 1.)은 앞서 소개한 국내외 양자 내성 암호 연구의 동향을 시간순으로 나열한 것이다. 이를 통해 양자 내성 암호의 연구가 활발히 이루어지고 있음을 알 수 있다.

2019년 정보통신계획평가원의 보고서에 따르면 유럽은 양자 정보 통신의 최고 기술 수준을 가진 국가로, 한국은 유럽과 비교하였을 때 상대적으로 81.3%의 기술 수준이다[14]. 이는 약 2년 동안의 기술격차로 다른 국가에 비해 가장 낮은 양자 암호 통신 기술 수준을 가지고 있음을 의미한다.

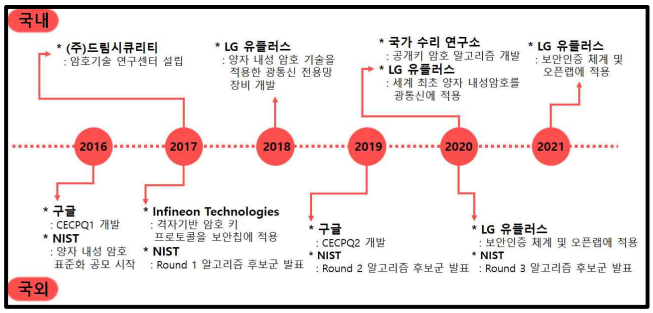

그림 1. 국내 양자 내성 암호 연구 동향

이렇듯 세계적으로 양자 내성 암호에 대한 연구는 활발히 진행되고 있지만, 아직 국내의 기술 수준은 선진국에 비해 미비한 상황이다. 이에 따라 양자 내성 암호에 대한 지속적인 관심을 가지고 선진국의 기술을 분석하여 현재 우리가 가지고 있는 기술을 적극적으로 보완해야 해야 한다.

Ⅴ. 결론

양자 컴퓨터의 발전으로 인해 기존의 암호 체계를 붕괴할 수 있는 다양한 양자 알고리즘이 등장하였다. 이에 따라 국내외 모두 양자 알고리즘으로부터 안전한 양자 내성 암호에 대한 활발한 연구가 진행 중이다.

본 논문에서는 양자 내성 암호의 국내외 연구 동향을 소개하였다. 국내의 경우, 현재 사용되고 있는 기성 암호 체계의 단점을 보완하고 양자 알고리즘으로부터 해독되지 않기 위한 새로운 암호 체계를 개발하여 실생활에 적용하는 등 양자 내성 암호의 적용 범위를 넓혀나가고 있다. 국외는 미국 국립 표준 기술 연구소를 기준으로 양자 내성 암호 표준화가 진행되고 있다. 이에 따라 향후 연구로 표준화 동향에 대해 분석하는 연구를 수행하고자 한다.

ACKNOWLEDGMENT

본 연구는 2021년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] Intel, "Moore's Law," Apr. 2021, (https://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html).

[2] 임승혁, "범용양자컴퓨터," 한국과학기술기획평가원, Dec. 2019.

[3] Grover, Lov K, "A fast quantum mechanical algorithm for database search," Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996.

[4] KISA report, "차세대 암호기술 '양자내성암호'와 '동형암호'," Jul. 2020.

[5] Hashnet, "양자내성암호," Mar. 2021, (http://wiki.hash.kr/index.php/양자내성암호).

[6] Shim, Kyung-Ah, et al, "A High-Speed Public-Key Signature Scheme for 8-b IoT-Constrained Devices," IEEE Internet of Things Journal 7(4), pp. 3663-3677, Apr. 2020.

[7] 국가수리과학연구소, "양자 컴퓨터에도 뚫리지 않는 고속 암호 기술 개발," Apr. 2020, (https://www.nims.re.kr/promote/post/media/33986).

[8] 김승한, "LGU+, 양자컴퓨터에 끄떡없는 새로운 암호기술 첫 적용," 매일경제, Jun. 2020, (https://www.mk.co.kr/news/it/view/2020/06/593408/).

[9] 이상오, "보안기술의 새바람 '양자컴퓨터'," 공학저널, Jul. 2020, (http://www.engjournal.co.kr/news/articleView.html?idxno=855).

[10] Wikipedia, "CECPQ2," Nov. 2020, (https://en.wikipedia.org/wiki/CECPQ2).

[11] 김영식, "NIST 양자 내성 암호 표준화 3라운드 알고리즘 특성 비교," 정보통신기획평가원, Dec. 2020.

[12] Infineon, "인피니언, 비접촉 보안칩에 포스트 양자 암호를 구현하여 2개의 "SESAMES Award" 수상," Nov. 2017, (https://www.infineon.com/cms/korea/kr/press/kor201711-30/).

[13] Infineon, "인피니언, 업계 최초로 비접촉 보안칩에 포스트 양자 암호 구현," Jun. 2017, (https://www.infineon.com/cms/korea/kr/press/KOR201706-03/).

[14] 이민경 외, "2019 ICT기술수준조사 및 기술경쟁력분석 보고서," 정보통신기획평가원, Jan. 2021.